WAITI'24 Program				
8:45	9:00	**Chairs Greetings**		
9:00	10:00	**Keynote**	The (In)Security of Machine Learning: The Road So Far	Stjepan Picek (Radboud University)
10:00	10:30	Coffe break		
10:30	12:00	**Session 1 - AI-Driven Cybersecurity Solutions for CTI, IoT and Software Infrastructures**		
		Paper 1	MIND-IoT: Machine Intelligence and Data-Mining for IoT Threats	**Kwabena B Aboagye-Otchere** (University of Texas Rio Grande Valley)*; Jorge Castillo (University of Texas Rio Grande Valley)
		Paper 2	A Privacy-Preserving Byzantine-Aware Swarm Learning Framework for CTI ***(online presentation)***	Marco Arazzi (University of Pavia); Dincy R Arikkat (Cochin University of Science and Technology); **Mert Cihangiroglu** (University of Pavia)*; Sameera K M (CUSAT)
		Paper 3	Automating AWS Security Controls: Leveraging Generative AI for Gherkin Script Generation	Mina Ghashami (Amazon)*; Nivedita Mangam (Amazon); Mohamadali Torkamani (Amazon Web Services); Felix Candela (Amazon); Bhavya Jain (Amazon); Farhan Diwan (Amazon); Malini SS (Amazon); Mingrui Cheng (Amazon); Chen Ling (Emory University); Ruslan Vaulin (Amazon); Kyuhong Park (AWS)
		Paper 4	The Rings of Tracking: Evaluating Security and Privacy in the Smart Ring Ecosystem	Johannes Ludwig (AWARE7 GmbH and Ruhr University Bochum); Veelasha Moonsamy (Ruhr University Bochum); **Matteo Große-Kampmann** (Rhine-Waal University of Applied Sciences and AWARE7 GmbH)*
12:00	13:30	Lunch		
13:30	15:00	*Paper 5*	Cyber Attack Detection for Internet of Health Things through Federated Deep Learning Technique	**Dr.Liyakath unisa** (Taibah University, Medinah, Saudi Arabia)*; Zoya Riyaz Syeda (Rajiv Gandhi University of Health Science); Riyaz Sohale Syed (Bangalore)
		Paper 6	MAD: A Meta-Learning Approach to Detect Advanced Persistent Threats using Provenance Data in Industrial IoT ***(online presentation)***	**Bikash Saha** (Indian Institute of Technology Kanpur)*; Nanda Rani (Indian Institute of Technology Kanpur); Sandeep K Shukla (IIT Kanpur)
		Session 2 - Leveraging Large Language Models for Cybersecurity and Threat Intelligence		
		Paper 7	Generating Abuse Stories and Misuse Cases using Large Language Models	Carmen Cheh (Illinois Advanced Research Center at Singapore Ltd.)*; **Nan Shing Kham Shing** (Singapore University of Technology and Design); Reuben Liang Yi Lim (Illinois Advanced Research Center at Singapore Ltd.); Binbin Chen (Singapore University of Technology and Design)
		Paper 8	Software Vulnerability Detection Using LLM: Does Additional Information Help? **(online presentation)**	**Samiha S Shimmi** (Northern Illinois Univesity)*; Yash Saini (Northern Illinois University); Mark Schaefer (Northern Illinois University); Hamed Okhravi (MIT Lincoln Laboratory); Mona Rahimi (Northern Illinois University)"
		Paper 9	Retrieval of Network Packets Information Using a Generated Latent Space Representation for Network Analysis in Cyber Security	Ofir Manor (Fujitsu Research of Europe); Ortal Lavi (Fujitsu Research of Europe); **Andres Murillo** (Fujitsu Research of Europe) *; Tomer Schwartz (Fujitsu Research of Europe); Ayoub M.A. M. Messous (FRE); Motoyoshi Sekiya (Fujitsu Research of Europe); Junichi Suga (Fujitsu Laboratories); Kenji Hikichi (Fujitsu Laboratories); Yuki Unno (Fujitsu Limited)
15:00	15:30	Coffe break		
15:30	17:00	*Paper 10*	Formal Trust and Threat Modeling Using Large Language Models	**Zhihao Yao** (New Jersey Institute of Technology)*
		Paper 11	Fine-tuning Large Language Models for DGA and DNS Exfiltration Detection ***(online presentation)***	**Md Abu Sayed** (University of Texas at El Paso)*; ASIF RAHMAN (UTEP); Christopher Kiekintveld (University of Texas at El Paso); Sebastian Garcia (Czech Technical University in Prague)
		Paper 12	Exploring Large Language Models for Semantic Analysis and Categorization of Android Malware	**Brandon Walton** (Louisiana State University); Mst Eshita Khatun (Louisiana State University); James Ghawaly (Louisiana State University); Aisha I Ali-Gombe (Louisiana State University)*
		Paper 13	Advancing TTP Analysis: Harnessing the Power of Large Language Models with Retrieval Augmented Generation	**Reza Fayyazi** (Rochester Institute of Technology)*; Rozhina Taghdimi (Rochester Institute of Technology); Shanchieh Yang (Gonzaga University)
		Closing Remarks and Presentation of Related Projects		
			CANARY (Cyber Analytics Network for Attribution and Reconnaissance Yield)" funded by Georgia Technology Research Institute (GTRI) under the Independent Research and Development (IRAD) program	Omar Alrawi (Georgia Tech, USA)
			SERICS (Security and Rights in CyberSpace - PE00000014) under the NRRP MUR program funded by the EU - NGEU	Serena Nicolazzo (University of Milan)
			PRIN 2022 Project HOMEY (Human-centric IoE-based Framework for Supporting the Transition Towards Industry 5.0 - 2022NX7WKE) funded by the EU - NGEU	Antonino Nocera (University of Pavia)
			OPTIMA (Organization sPecific Threat Intelligence Mining and sharing - 101063107) partly supported by HORIZON Europe Framework Programme	Vinod P. (University of Padua)